BAB II

LANDASAN TEORI

2.1 Quality of Service (QoS)

Dalam mengukur *Quality of Service* (QoS) tidak ada satu standarisasi tentang bagaimana model QoS yang baik. *IETF Internet Protocol Performance Metrics* (IPPM) mencoba mendefinisikan satuan ukur (*metrics*) untuk *internet performance* yang merupakan awal dari pengukuran performa internet

2.6.1 Defenisi QoS

Quality of Service (QoS) merupakan totalitas dari karakteristik layanan telekomunikasi yang bertanggung jawab terhadap kemampuannya untuk memuaskan kebutuhan pengguna layanan tersebut, baik secara tersirat maupun dinyatakan (ITU-T Recommendation, 2008).

QoS mengacu kepada kemampuan suatu sistem terdistribusi untuk menyediakan layanan komputasi dan jaringan seperti harapan masing-masing pengguna untuk memenuhi kualitas dan ketepatan waktu (Irvine, dkk, 2000).

QoS mencakup semua aspek dari sebuah koneksi, antara lain *service response time*, *packet loss*, *signal to noise ratio*, *cross talk*, *echo*, *interrupt*, *frequency response*, dan lain-lain.

2.6.2 Terminologi QoS

Terminologi QoS diklasifikasikan ke dalam 3 area, antara lain layanan (*service*), jaringan (*network*) dan manajemen (*management*) .

a. QoS yang berhubungan dengan kualitas layanan (*service*) terdiri dari kecepatan pemrosesan (*speed*), tingkat ketepatan (*accuracy*), tingkat kepastian atau jaminan (*dependability*), ketersediaan (*availability*), keandalan (*reliability*), kemudahan (*simplicity*) dan sebagainya.
b. QoS yang berhubungan dengan jaringan (*network*) terdiri dari *network accessibility*, *connection accessibility*, *connection error probability*, *connection failure probability*, *misrouting probability*, *bit error ratio*, *transmission performance* dan sebagainya.

c. QoS yang berhubungan dengan manajemen (*management*) terdiri dari *resource management, class of service, customer relationship management, benchmark, service level agreement, time between interruptions, interruption duration, mean time between interruption, mean time to restoration, fault coverage, repair coverage, maintenance, disaster recovery, complaint, directory service* dan sebagainya.

2.2 Kualitas Jaringan

Pada jaringan terdapat berbagai faktor yang mempengaruhi kualitas jaringan antara lain faktor manusia dan faktor teknis. Faktor manusia terdiri dari kestabilan layanan (*stability of service*), ketersediaan layanan (*availability of service*), jeda waktu (*delay*), informasi pengguna dan lain-lain (Peuhkuri dan Markus, 1999).

Sedangkan faktor teknis terdiri dari keandalan (*reliability), scalability, effectiveness, maintainability, grade of service* dan lain-lain.

Transmisi sebuah paket data yang melewati jaringan dari transmiter sampai receiver akan mengalami berbagai permasalahan, di antaranya:

a. Utilisasi/Okupansi

Teknologi IP adalah teknologi *connectionlessoriented*, dimana proses transmisi informasidari pengirim ke tujuannya tidak memerlukanpendifinisian jalur terlebih dahulu, sepertihalnya teknologi *connection oriented*.

Dalam hal ini *Utilisasi/okupansi* jaringancenderung dipengaruhi langsung oleh trafikyang ditransmisikan melewati jaringan *IP*tersebut. Sebagai gambaran pada tabel di bawahini, menunjukkan besarnya *bytes* yangdiperlukan untuk proses aplikasi *IP*.

Tabel 2.1 Ukuran paket di dalam setiap Aplikasi (Sumber *TIPHON-Telecommunicationsand)*

Application	Packet Size
Telnet	64-1518 bytes
http	400-1518 bytes
NFS	64-1518 bytes
Netware	500-1518 bytes
Multimedia	400-700 bytes

Utilisasi/Okupansi IP yang dinyatakan dalampersen, dapat dihitung sebagai berikut :

$$Ip\ Occupancy = \frac{average\ t\ \ roug\ \ put\ of\ ip\ traffic}{bandwitc\ \ \ capacity\ of\ p\ \ isacal\ link} \times 100\%$$

Seiring dengan perkembangan di teknologijaringan *IP* dan kebutuhan dari layanan yangjalan di jaringan tersebut, layanan di jaringan*IP* tidak lagi hanya mengenal kelas *Best Effort*.Jaringan *IP* sudah dapat melakukan pengolahantrafik sesuai permohonan dari pelangganataupun disesuaikan dengan permintaan darisuatu layanan. Pengelolaan *traffic* ini dikenaldengan *QoS (Quality of Service)*. *QoS* dijaringan dapat dikelompokan terdiri atasbeberapa kelas layanan, mulai dari kelas *BestEffort*, kelas *real time* (terutama dipergunakanoleh layanan yang memerlukan pengiriman *traffic* yang *real time*), kelas yang membagiatas trafik yang dijamin dan *best effort*.

b. Throughput

Throughput adalah *bandwidth* aktual yang terukur pada suatu ukuran waktu tertentu dalam suatu hari menggunakan rute internet yang spesifik ketika sedang mendownload suatu file

Throughput akan dipengaruhi oleh tipe *data-stream* pada jaringan. Tipe *data-stream* tertentu bisa saja membutuhkan prioritas lebih tinggi dalam jaringan jika dibandingkan dengan tipe *data-stream* lain. Misalkan data multimedia (video dan audio)

c. Packets Loss

Packet loss didefinisikan sebagai kegagalantransmisi paket IP mencapai tujuannya.Kegagalan paket tersebut mencapai tujuan,dapat disebabkan oleh beberapa kemungkinkan,diantaranya yaitu

1. Terjadinya *overload* trafik didalam jaringan
2. Tabrakan (*congestion*) dalamjaringan
3. *Error* yang terjadi pada media fisik
4. Kegagalan yang terjadi pada sisipenerima antara lain bisa disebabkan karena*overflow* yang terjadi pada *buffer*.

Di dalam implementasi jaringan *IP*, nilai*packet loss* ini diharapkan mempunyai nilaiyang minimum. Secara umum terdapatempat kategori penurunan performansijaringan berdasarkan nilai *packet loss*

sesuaidengan versi *TIPHON-Telecommunicationsand Internet ProtocolHarmonization OverNetworks* (Joesman 2008), yaitu sepertitampak pada tabel berikut.

Tabel 2.2 Ukuran paket di dalam setiap Aplikasi (*TIPHON-Telecommunicationsand}*

Kategori Degredasi	Packet Loss
Sangat Bagus	0
Bagus	3%
Sedang	15%
Jelek	25%

d. Delay

Delay adalah waktu tunda suatu paket yangdiakibatkan oleh proses transmisi dari satu titikke titik lain yang menjadi tujuannya. *Delay* didalam jaringan dapat digolongkan sebagaiberikut :

1. *Packetisasi delay*

   Delay yang disebabkan oleh waktu yangdiperlukan untuk proses pembentukan paket*IP* dari informasi user. *Delay* ini hanya terjadi sekali saja, yaitu di *source* informasi.

$$Packetization\ delay = \frac{payload\ size\ of\ IP}{source\ information\ rate}$$

2. *Quening Delay*

   Delay ini disebabkan oleh waktu proses yangdiperlukan oleh *router* di dalam menanganitransmisi paket di sepanjang jaringan.Umumnya *delay* ini sangat kecil, kurang lebih sekitar 100 *micro second*.

3. *Delay* Propagasi

   Proses perjalanan informasi selama di dalammedia transmisi, misalnya *SDH*, *coax* atautembaga, menyebabkan *delay* yang disebut dengan *delay propagasi.*

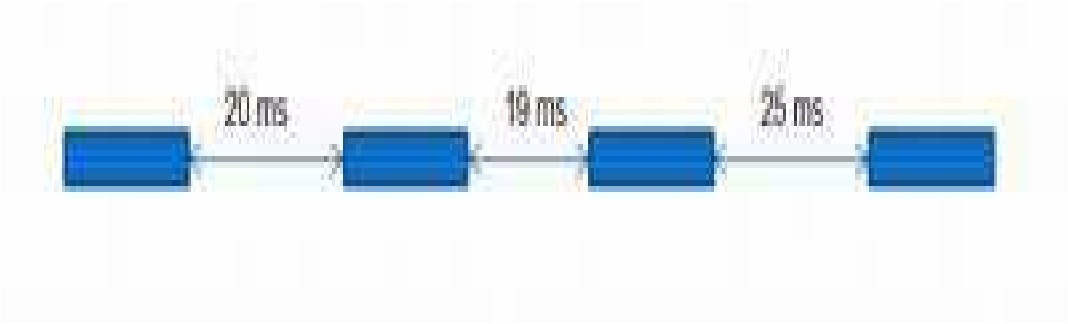
Menurut versi *TIPHON* (Joesman 2008)besarnya *delay* dapat diklasifikasikasebagai berikut :

Tabel 2.3Perfomansi Jaringan IP berdasarkan Delay/latency (*TIPHON)*

Kategori Latency	Besar Delay
Sangat Bagus	< 150 ms
Bagus	150 – 300 ms
Sedang	300 – 450 ms
Jelek	>450 ms

e. Jitter

Jitter merupakan variasi *delay* antar paket yangterjadi pada jaringan *IP*. Besarnya nilai *jitter*akan sangat dipengaruhi oleh variasi bebantrafik dan besarnya tumbukan antar paket(*congestion*) yang ada dalam jaringan *IP*.Semakin besar beban trafik di dalam jaringanakan menyebabkan semakin besar pula peluangterjadinya *congestion* dengan demikian nilai*jitter*-nya akan semakin besar. Semakin besarnilai *jitter* akan mengakibatkan nilai *QoS* akan semakin turun.ini akan sangat berpengaruh terhadap kualitas *streaming* audio atau video.



Gambar 2.1 Contoh *Jitter* (TIPHON)

Untuk mendapatkan nilai *QoS*jaringan yang baik, nilai *jitter* harus dijagaseminimum mungkin. Terdapat empat kategoripenurunan performansi jaringan berdasarkannilai *peak jitter* sesuai dengan versi *TIPHON*(Joesman 2008), yaitu :

Tabel 2.4 Perfomansi Jaringan IP berdasarkan Jitter (*TIPHON}*

Kategori Jitter	Besar Jitter
Sangat Bagus	0

Bagus	1 – 75ms
Sedang	76 – 125ms
Jelek	126 – 225 ms

f. Out of order delivery

Hal ini terjadi apabila suatu paket yang dikirimkan melalui *router* yang berbeda, memungkinkan untuk sampai pada tujuan dan mengakibatkan paket diterima tidak sesuai dengan urutan paket yang dikirim.

g. Out of order delivery

Hal ini terjadi apabila suatu paket yang dikirimkan melalui *router* yang berbeda, memungkinkan untuk sampai pada tujuan dan mengakibatkan paket diterima tidak sesuai dengan urutan paket yang dikirim.

2.3 QoS pada IP *Network*

Untuk menyediakan QoS pada *IP Network,IP R*outer perlu dilengkapi dengan berbagai fungsi tambahan. Pertama, sebuah *host* harus melakukan *resource reservation* pada *router* sepanjang jalur menuju tempat pengiriman melalui *signaling protocol*. *Request* tersebut akan melalui sebuah rute dimana router dapat menawarkan jalur terbaik, yang disebut dengan *QoS Routing*. Setiap router sepanjang jalur melakukan *admission control* untuk menentukan apakah *request* tersebut diterima atau ditolak.

Apabila permintaan *resource reservation* tersebut diterima, maka router akan siap untuk menerima aliran data dari *host*. Pada saat aliran data dikirim dan diterima oleh *router*, *router* perlu melakukan *classifying* terhadap semua paket yang diterima menjadi per-*flowqueue* atau per-*class queue*, lalu menerapkan *policing* untuk melihat apakah paket tersebut menggunakan *resource* yang berlebihan dari *resource* yang diminta, dan terakhir melakukan *scheduling* untuk memastikan paket tersebut mendapatkan alokasi *bandwidth*

2.4 Komponen QoS

Terdapat 6 komponen yang perlu diperhatikan dalam membangun jaringan yang memilki QoS, antara lain :

a. Signaling Protocol

Merupakan protokol umum yang digunakan untuk melakukan komunikasi antar *router* dengan tujuan untuk *resource reservation*. Salah satu protokol

yang sering digunakan adalah *Resource ReserVation Protocol* (RSVP) yang digunakan oleh aplikasi untuk melakukan reservasi terhadap *resource* pada suatu jaringan. Contoh lain adalah protokol *Common Open Policy Service* (COPS), yaitu protokol *query-response* yang sederhana yang digunakan di dalam *policy management system* yang merupakan bagian dari arsitektur *QoS Management*.

b. QoS Routing

QoS Routing menyediakan rute yang dinamis yang ditentukan berdasarkan waktu dan panjang jalur. *Router* melakukan pemilihan rute berdasarkan informasi dasar seperti jumlah hop yang sedikit, *delay*, *bandwidth*, *loss ratio* dan lain-lain.

c. Admission Control

Pemilihan rute yang terdekat akan memungkinkan terjadinya kemacetan di suatu jalur tertentu, untuk itu perlu adanya *admission control* yang mengatur apakah paket tersebut boleh melewati rute tersebut atau tidak. Hal ini ditentukan berdasarkan jumlah paket yang menumpuk pada jalur tersebut, apabila jalur tersebut dipadati dengan paket yang sedang menunggu antrian (macet), maka paket akan di-*drop*.

d. Packet Classification

Apabila jalur telah disepakati, melalui *signaling protocol*, *QoS Routing* dan *Admission Control*, maka paket dapat dikirimkan ke tujuan. Paket perlu diklasifikasikan.

e. Policing

Komponen ini mengatur hak-hak paket. Apakah paket tersebut menggunakan *resource* yang berlebihan dari yang disepakati. Jika paket tersebut melebihi penggunaan *resource*-nya, maka paket tersebut akan di-*drop* atau diberi jeda waktu (*delay*).

f. Scheduling

Tujuan umum adalah untuk melakukan *resource sharing* antara kelas paket. Terdapat bermacam-macam algoritma yang digunakan untuk *scheduling*, mulai dari yang sederhana sampai yang rumit.

2.5 Arsitektur QoS

Terdapat 2 arsitektur dari QoS antara lain *Integrated Services* (IntServ) dan *Differential Services* (DiffServ).

a. *Integrated Services* (IntServ)

   Merupakan arsitektur yang lengkap yang dapat memenuhi hampir seluruh kebutuhan QoS yang disebabkan oleh *critical network applications*. Namun IntServ memerlukan *cost* yang besar.

b. *Differential Services* (DiffServ)

   Merupakan solusi sederhana dengan menyediakan layanan yang berbeda berdasarkan level pengguna. Perbedaan layanan tersebut mencakup *bandwidth*, *delay* dan lain-lain

2.6 *Mobile Ad-Hoc Network* (MANET)

Pada bagian ini akan membahas tetang *Mobile Ad- Hoc Network* (MANET) secara lengkap.

2.6.1 Definisi MANET

Mobile Ad Hoc Network (MANET) adalah kumpulan dari beberapa wireless node yang dapat di *set-up* secara dinamis dimana saja dan kapan saja tanpa menggunakan infrastruktur jaringan yang ada .MANET juga merupakan jaringan sementara yang dibentuk oleh beberapa *mobile node* tanpa adanya pusat administrasi dan infrastruktur kabel .Pada MANET, *mobile host* yang terhubung dengan *wireless* dapat bergerak bebas dan juga berperan sebagai router.

Terdapat beberapa perbedaan antara jaringan *ad hoc* dengan jaringan yang memiliki infrastruktur, antara lain :

a. *Peer-to-Peer*, yaitu komunikasi antara dua node dalam satu *hop*.
b. *Remote-to-Remote*, yaitu komunikasi antar dua *node* diluar satu *hop*, namun masih tetap mengelola kestabilan rute di antara keduanya.
c. *Dynamic Traffic*, terjadi ketika *node* bergerak, maka rute harus dikonstruksi ulang. Ini merupakan hasil dari tingkat konektifitas yang rendah.

2.6.2 Karakteristik MANET

Berdasarkan dokumen *Request for Comments* menjelaskan bahwa terdapat beberapa karakteristik dari *Mobile Ad Hoc Network* (MANET). Disana dijelaskan

bahwa MANET terdiri dari *mobile platform* (seperti router dan perangkat *wireless*) dalam hal ini disebut dengan "*node*" yang bebas berpindah-pindah ke mana saja. *Node* tersebut bisa saja berada di pesawat, kapal, mobil dan dimana saja(Corson, S. dan Macker, J, 1999).

Setiap *node* dilengkapi dengan *transmitter* dan *receiver wireless* menggunakan antena atau sejenisnya yang bersifat *omnidirectional* (*broadcast*), *highly directional* (*point to point*), memungkinkan untuk diarahkan, atau kombinasi dari beberapa hal tersebut. *Omnidirectional* maksudnya adalah gelombang radio dipancarkan ke segala arah oleh perangkat *transmitter wireless*. Sedangkan *highly directional* adalah gelombang dipancarkan ke satu arah tertentu(Corson, S. dan Macker, J, 1999).

Selain karakteristik di atas, *Mobile Ad Hoc Network* (MANET) juga memiliki beberapa karakteristik yang lebih menonjol, antara lain (Corson, S. dan Macker, J, 1999):

a. Topologi yang dinamis : *Node* pada MANET memiliki sifat yang dinamis, yaitu dapat berpindah-pindah kemana saja. Maka topologi jaringan yang bentuknya adalah loncatan antara *hop* ke *hop* dapat berubah secara tidak terpola dan terjadi secara terus menerus tanpa ada ketetapan waktu untuk berpindah. Bisa saja didalam topologi tersebut terdiri dari *node* yang terhubung ke banyak *hop* lainnya, sehingga sangat berpengaruh secara signifikan terhadap susunan topologi jaringan.
b. Otonomi : Setiap *node* pada MANET berperan sebagai *end-user* sekaligus sebagai router yang menghitung sendiri *route-path* yang selanjutnya akan dipilih.
c. Keterbatasan *bandwidth* : Link pada jaringan *wireless* cenderung memiliki kapasitas yang rendah jika dibandingkan dengan jaringan berkabel. Jadi, kapasitas yang keluar untuk komunikasi *wireless* juga cenderung lebih kecil dari kapasitas maksimum transmisi. Efek yang terjadi pada jaringan yang berkapasitas rendah adalah *congestion* (kemacetan).
d. Keterbatasan energi : Semua *node* pada MANET bersifat *mobile*, sehingga sangat dipastikan *node* tersebut menggunakan tenaga baterai untuk beroperasi. Sehingga perlu perancangan untuk optimalisasi energi.

Keterbatasan Keamanan : Jaringan *wireless* cenderung lebih rentan terhadap keamanan daripada jaringan berkabel. Kegiatan pencurian (*eavesdroping*, *spoofing* dan *denial of service*) harus lebih diperhatikan.

2.6.3 Protokol MANET

Terdapat berbagai jenis protokol routing untuk MANET yang secara keseluruhan dapat dibagi menjadi beberapa kelompok, antara lain :

a. Proactive Routing

Algoritma ini akan mengelola daftar tujuan dan rute terbaru masing-masing dengan cara mendistribusikan *routing table* ke seluruh jaringan,sehingga jalur lalu lintas (*traffic*) akan sering dilalui oleh *routing table* tersebut. Hal ini akan memperlambat aliran data jika terjadi restrukturisasi *routing table*. Salah satu *proactive routing* yang digunakan adalah *OLSR – Optimized Link State Routing Protocol. Protokol Optimized Link State Routing (OLSR)* merupakan optimalisasi dari protokol *link state* yang dasar. Protokol ini menggunakan konsep *multipoint relays (MPRs)* untuk mengurangi ukuran kapasitas control messages. Dengan adanya konsep MPRs, maka protokol ini dapat memperkecil terjadinya *flooding* terhadap lalu lintas *control messages*.

Terdapat dua fungsionalitas utama dari OLSR, yaitu *Neighbor Discovery* dan *Topology Dissemination. Neighbor Discovery* merupakan fungsi untuk menemukan siapa *node* yang berada di dekat *node* tersebut dengan cara mengirimkan pesan "*hello*" secara *broadcast* dalam waktu *interval* tertentu, yang disebut hello interval. Sedangkan *Topology Dissemination* merupakan bentuk penyebaran informasi topologi ke semua *node* secara *broadcast.* Pengiriman informasi ini dilakukan secara berkala, sehingga akan membanjiri jalur lalu lintas data. Pada OLSR, pengiriman informasi topologi hanya dilakukan kepada *two-hop node* atau *multipointrelays*. Sehingga akan mencegah pengiriman informasi topologi yang tidak diperlukan.

b. Reactive Routing

Tipe ini akan mencari rute (*on demand*) dengan cara membanjiri jaringan dengan paket *router request.* Sehingga dapat menyebabkan jaringan akan

penuh (*clogging*), salah satunya *Ad Hoc On Demand Distance Vector* (AODV). AODV adalah *distance vector routing protocol* yang termasuk dalam klasifikasi reaktif *routing protocol*, yang hanya me-request sebuah rute saat dibutuhkan. AODV yang standar ini dikembangkankan oleh C. E. Perkins, E.M. (Belding-Royer dan S. Das)

Ciri utama dari AODV adalah menjaga *timer-based state* pada setiap *node* sesuai dengan penggunaan table *routing*. Tabel *routing* akan kadaluarsa jika jarang digunakan. AODV memiliki *route discovery* dan *route maintenance*. *Route Discovery* berupa *Route Request* (RREQ) dan *Route Reply* (RREP). Sedangkan *Route Maintenance*berupa Data, *Route update* dan *Route Error* (RRER).

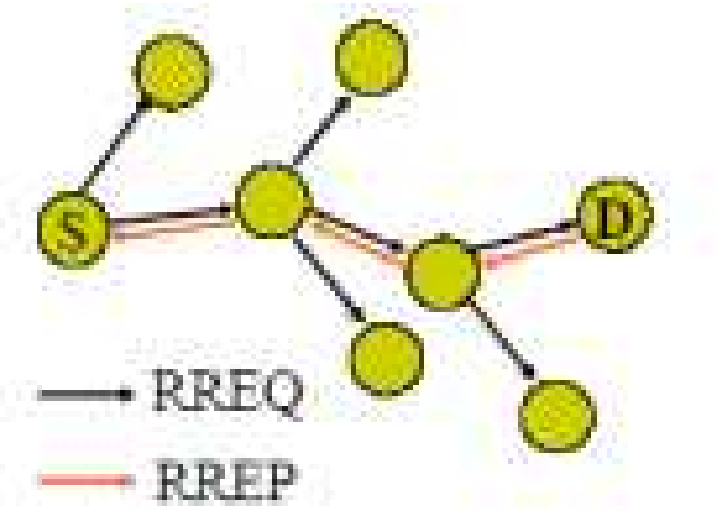
AODV memerlukan setiap *node* untuk menjaga tabel *routing* yang berisi :

a. *Destination IP Address*: berisi alamat IP dari *node*tujuan yang digunakan untuk menentukan rute.
b. *Destination Sequence Number* : *destination sequence number* bekerjasama untuk menentukan rute
c. *Next Hop*: 'Loncatan' (*hop*) berikutnya, bisa berupa tujuan atau *node* tengah, *field* ini dirancang untuk meneruskan paket ke *node* tujuan.
d. *Hop Count*: Jumlah *hop* dari alamat IP sumber sampai ke alamat IP tujuan.
e. *Lifetime:* Waktu dalam milidetik yang digunakan untuk *node* menerima RREP.
f. *Routing Flags*: Status sebuah rute; *up (valid), down* (tidak valid) atau sedang diperbaiki.

AODV mengadopsi mekanisme yang sangat berbeda untuk menjaga informasi *routing*. AODV menggunakan tabel *routing* dengan satu *entry* untuk setiap tujuan. Tanpa menggunakan *routing* sumber, AODV mempercayakan pada tabel *routing* untuk menyebarkan *RouteReply* (RREP) kembali ke sumber dan secara sekuensial akan mengarahkan paket data menuju ketujuan. AODV juga menggunakan *sequence* numberuntuk menjaga setiap tujuan agar didapat informasi routing

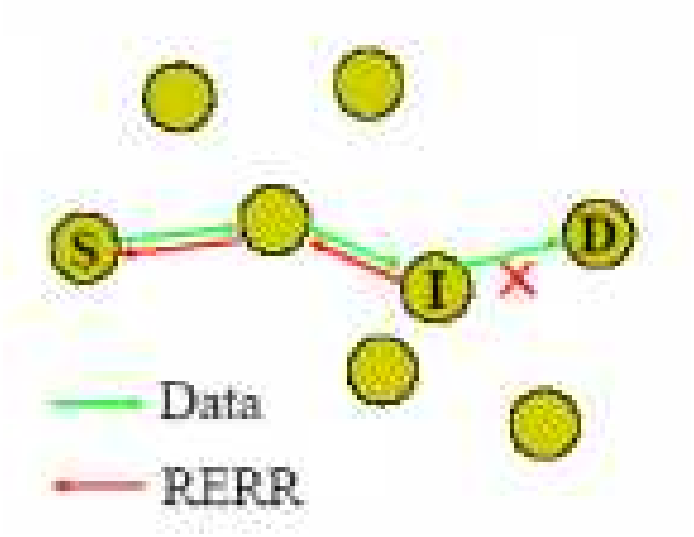
yang terbaru dan untuk menghindari *routing loops*. Semua paket yang diarahkan membawa *sequence number* ini.

Penemuan jalur (*Path discovery*) atau *Route disco*very di-inisiasi dengan menyebarkan *RouteReply* (RREP), seperti terlihat pada



Gambar 2.*2 Routing Flag* AODV (www.wikipedia.org)

Ketika RREP menjelajahi *node*, ia akan secara otomatis men-*setup path*. Jika sebuah *node* menerima RREP, maka nodetersebut akan mengirimkan RREP lagi ke *node* atau *destination sequence number*. Pada proses ini, *node*pertama kali akan mengecek *destination sequence*pertama kali akan mengecek *destination sequencenumber* pada tabel *routing*, apakah lebih besar dari 1 (satu) pada *RouteRequest*(RREQ), jika benar, maka *node* akan mengirim RREP. Ketika RREP berjalan kembali ke *source* melalui *path* yang telah di-*setup*, ia akan men-*setup* jalur kedepan dan meng-*update timeout*. Jika sebuah *link* ke *hop* berikutnya tidak dapat dideteksi dengan metode penemuan rute, maka *link* tersebut akan diasumsikan putus dan *RouteError* (RERR) akan disebarkan ke *node* tetangganya seperti terlihat pada Gambar 3. Dengan demikian sebuah *node* bisa menghentikan pengiriman data melalui rute ini atau meminta rute baru dengan menyebarkan RREQ kembali.



Gambar 2.3 Mekanisme data *Route Update*(www.wikipedia.org)

2.6.4 Fokus Pengembangan MANET

Topik tentang *Mobile Ad Hoc Network* (MANET) menjadi sangat banyak dijadikan penelitian. Adapun fokus penelitian MANET saat ini mengacu kepada beberapa hal antara lain (Sun, Jun-Zhao,2001):

a. Routing

Topologi MANET yang secara dinamis dapat berubah-ubah menyebabkan muncul tantangan untuk mencari solusi untuk *routing* paket. Hal ini penting karena pada saat ada perubahan posisi *node*, maka kemungkinan besar jalur *routing* akan berubah dan perlu untuk mengatur ulang jalur *routing*.

b. *Security* dan *Reliability*

Keamanan sangat diperlukan terlebih pada jaringan *wireless*. Ini akan mencegah seseorang untuk mengambil dan mengirimkan paket yang tidak diinginkan. Selain itu juga terhadap ketangguhan jaringan *wireless* yang memiliki jangkauan yang terbatas.

c. *Quality of Service* (QoS)

Penerapan QoS pada jaringan yang selalu berubah-ubah merupakan tantangan tersendiri. Implementasi QoS harus dikembangkan agar dapat menyesuaikan dengan kondisi jaringan pada MANET.

d. Internetworking

Selain komunikasi antar *node* di dalam MANET, juga perlu mengembangkan teknologi untuk berkomunikasi pada jaringan tetap.

e. *Power Consumption*

Hampir sebagian besar perangkat *mobile* saat ini menggunakan baterai sebagai sumber dayanya. Untuk penggunaan dalam jangka waktu yang relatif lama, maka perlu dikembangkan cara memperpanjang waktu operasi perangkat tersebut dengan cara memperbesar kapasitas baterai atau memperkecil jumlah konsumsi baterai

2.6.5 Kebutuhan QoS Pada MANET

Dikarenakan karakteristik dari MANET yang berbeda dengan jaringan tetap, maka dalam menerapkan QoS pada MANET perlu memperhatikan beberapa hal berikut ini :

a. *Route Stability*

Kestabilan *routing* haruslah dijaga mengingat karakteristik topologi MANET yang dapat berubah-ubah menyebabkan rekonstruksi jalur *routing* setiap saat khususnya pada saat terjadi perubahan *node*.

b. *Security*

Keamanan data harus menjadi perhatian karena data mengalir melalui jaringan *wireless* yang sangat mudah untuk direkam. Penggunaan enkripsi yang kuat akan membantu meningkatkan keamanan pada jaringan tersebut.

c. *Reliability*

Keandalan jaringan menjadi perhatian penting karena jaringan dibangun menggunakan media gelombang radio yang memiliki keterbatasan jangkauan dan mudah terjadinya tabrakan gelombang (interferensi) yang menyebabkan terjadinya *bit-error* atau paket yang rusak dalam perjalanan